HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN QUANG ANH

NGHIÊN CỨU KỸ THUẬT TẤN CÔNG MẠNG NỘI BỘ VÀ PHƯƠNG PHÁP PHÒNG CHỐNG

Chuyên ngành: KHOA HỌC MÁY TÍNH

Mã số: 8.48.01.01

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - NĂM 2022

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS.TS. ĐỖ XUÂN CHỢ

Phản biện 1: TS. Vũ Văn Thỏa

Phản biện 2: PGS.TS. Đặng Văn Đức

Luận văn được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông.

Vào lúc: 09 giờ 00 ngày 17 tháng 02 năm 2023

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

1. Lý do chọn đề tài

Trong những năm gần đây, sự phát triển nhanh chóng của ngành Công nghệ thông tin (CNTT) đã mang lại nhiều tiện ích trong cuộc sống. Mọi công việc trở nên nhẹ nhàng, nhanh chóng và tiện lợi hơn nhờ số hóa. Ứng dụng của CNTT được áp dụng vào hầu hết các công việc hàng ngày, từ đi chợ, mua sắm hàng hóa, học tập, làm việc, các dịch vụ công. Rất nhiều doanh nghiệp, cơ quan nhà nước đã và đang tiến hành chuyển đổi số, nhằm đem các ứng dụng CNTT vào phục vụ công việc một cách triệt để. Tuy nhiên, cùng với những lợi ích đó, sự phát triển của CNTT cũng mang đến một loại hình tội phạm mới – tội phạm sử dụng công nghệ cao. Ví dụ điển hình là những vụ tấn công vào các hệ thống máy chủ, cài cắm mã độc, virus, mã hóa các thông tin nhạy cảm để đòi tiền chuộc, hoặc nguy hiểm hơn là xâm phạm an ninh quốc phòng. Các hình thức tấn công mạng ngày càng tinh vi hơn, và không chỉ trên môi trường Internet, những hệ thống mạng nội bộ, mạng diện rộng dùng đường truyền riêng cũng có nguy cơ bị tấn công rất cao.

Đối với các công ty lớn, việc bị tấn công mạng nội bộ có thể gây thiệt hại lớn về mặt tiền bạc, còn đối với các cơ quan nhà nước, mức độ thiệt hại có thể lớn hơn rất nhiều, thậm chí có thể ảnh hưởng tới nền an ninh Quốc gia. Chính vì thế, việc nghiên cứu về các phương pháp tấn công mạng, cũng như các biện pháp để phòng thủ là vô cùng cần thiết và là nhu cầu cấp bách hiện nay. Từ những lý do như vậy, học viên lựa chọn đề tài: "**NGHIÊN CỨU KỸ THUẬT TẤN CÔNG MẠNG NỘI BỘ VÀ PHƯƠNG PHÁP PHÒNG CHỐNG**".

2. Tổng quan về đề tài nghiên cứu

Hiện nay các phương pháp tấn công mạng và cách ngăn chặn được phổ biến khá nhiều trên Internet, một người có chút ít kiến thức về CNTT cũng có thể tự học cách tấn công mạng trên YouTube. Tuy nhiên, hầu hết các phương pháp này đều áp dụng trên nền tảng Internet, và đối tượng chủ yếu là người dùng cuối, với các mục tiêu như cài mã quảng cáo, điều hướng người dùng đến trang web giả mạo, virus mã

hóa đòi tiền chuộc, lấy thông tin cá nhân, thẻ tín dụng, tài khoản ngân hàng. Còn đối với các mạng nội bộ, không có kết nối Internet, hoặc kết nối một phần với Internet thì các phương pháp tấn công và phòng thủ lại có sự khác biệt. Khác biệt từ các phương pháp tấn công, mục tiêu tấn công và mục đích tấn công.

Đối với các cơ quan, doanh nghiệp sử dụng mạng nội bộ thường thiếu sự phòng bị và đầu tư liên quan đến việc chống tấn công mạng. Lý do chính là chủ quan về việc không kết nối Internet thì không thể tấn công được. Quan niệm trên là không chính xác, các phương pháp tấn công mạng nội bộ vẫn có thể thực hiện được dù không có kết nối tới Internet, hoặc thông qua các vùng trung gian giữa mạng nội bộ và Internet, hoặc thông qua các thiết bị ngoại vi, như USB, đĩa CD,…. Mặt khác, đa phần các vụ tấn công mạng đều xảy ra rồi thì phía nạn nhân mới biết, nên thường rơi vào tình trạng bị động, lo khắc phục sự cố. Chính vì thế cần có những giải pháp để có thể chủ động chống tấn công, phát hiện trong quá trình tấn công, tránh việc luôn phải đi sau để dọn dẹp hậu quả.

Đề tài nghiên cứu các phương pháp tấn công mạng nội bộ và phương pháp phòng chống sẽ tập trung vào phân tích khái quát về mạng nội bộ, phân tích các phương pháp tấn công qua mạng LAN đồng thời chỉ ra các điểm mạnh, điểm yếu của phương pháp đó và cách để phòng thủ hiệu quả nhất. Cùng với đó là nghiên cứu một số phương pháp chống tấn công chủ động.

3. Mục đích nghiên cứu

- Tìm hiểu về mạng nội bộ.
- Nghiên cứu một số kỹ thuật tấn công mạng nội bộ và phương pháp chống tấn công mạng nội bộ.
- Nghiên cứu một số phương pháp để chủ động phòng chống tấn công mạng nội bộ.
- Xây dựng mô hình thử nghiệm, lên kịch bản và tiến hành tấn công, phòng chống.

4. Đối tượng và phạm vi nghiên cứu

- Đối tượng: mạng nội bộ mạng diện rộng của doanh nghiệp lớn, cách phòng chống và giải pháp chủ động chống tấn công.
- Phạm vi: một số kỹ thuật tấn công mạng nội bộ và cách phòng chống.

5. Phương pháp nghiên cứu

Luận văn tập trung vào nghiên cứu và tìm hiểu về lý thuyết của các kỹ thuật tấn công. Bên cạnh đó là khai thác sử dụng một số phần mềm máy tính. Và cuối cùng là thực nghiệm trên mô hình mạng.

6. Cấu trúc của luận văn

- Chương 1 trình bày Tổng quan về mạng nội bộ
- Chương 2 tấn công mạn nội bộ và giải pháp chống tấn công
- Chương 3 thực nghiệm và đánh giá

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG NỘI BỘ

1.1. Giới thiệu về mạng nội bộ

1.1.1. Mạng nội bộ là gì

Một mạng nội bộ là một mạng riêng cho các cá nhân của một tổ chức. Thông thường, một loạt thông tin và dịch vụ có sẵn trên mạng nội bộ của một tổ chức không được công khai cho tất cả mọi người, không giống như Internet.

Hình 1.1. Mạng nội bộ

1.1.2. Cách sử dụng trong hệ thống mạng nội bộ

Ngày nay, mạng nội bộ đang được sử dụng để cung cấp các công cụ, tính năng, ví dụ như cộng tác để tạo điều kiện làm việc theo nhóm và hội nghị trực tiếp, hoặc các thư mục công ty, các công cụ quản lý sản phẩm , quản lý dự án , v.v..

Hình 1.2. Cách sử dụng trong hệ thống mạng nội bộ

1.1.3. Lợi ích của hệ thống mạng nội bộ

- Năng suất lao động, linh hoạt về thời gian, giao tiếp dễ dàng, cải thiện quy trình làm việc, tiết kiệm về chi phí.
- Đa nền tảng và dễ cập nhật ngay lập tức.

1.2. Công nghệ truyền dẫn mạng dây Ethernet

1.2.1. Khái niệm về Ethernet

Ethernet là một công nghệ mạng truyền gồm các công nghệ mạng dựa trên khung dữ liệu (frame-based) dành cho mạng LAN.

1.2.2. Ethernet là một công nghệ mạng thiết bị và rộng rãi

Ngày nay mặc dù có nhiều công nghệ LAN ra đời nhưng Ethernet vẫn là công nghệ được sử dụng rộng rãi nhất. Vào năm 1993, các nhà phân tích đã thống kê có khoảng hơn 45 triệu nút mạng Ethernet đã và đang được sử dụng trên toàn thế giới.

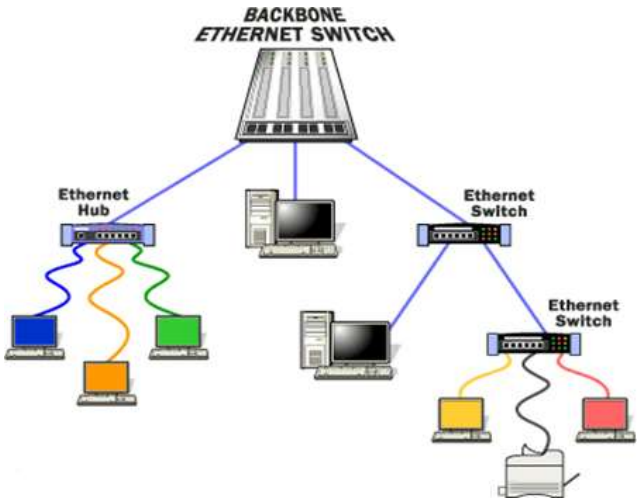
1.2.3. Lịch sử phát triển của Ethernet

Ethernet đã được phát minh ra tại trung tâm nghiên cứu Xerox Palo Alto vào những năm 1971 bởi tiến sĩ Robert M. Metcalfe. Ban đầu, Ethernet được thiết kế với mục đích chính là phục vụ nghiên cứu trong hệ thống quản lý công ty.

1.2.4. Các thành phần của Ethernet

Hệ thống Ethernet bao gồm 3 thành phần cơ bản :

- Ở hệ thống ở trung gian truyền tín hiệu Ethernet giữa các máy tính với nhau.
- Nhóm thiết bị trung gian sẽ đóng vai trò là giao diện Ethernet làm cho nhiều máy tính có thể kết nối tới cùng 1 kênh.
- Còn các khung Ethernet sẽ đóng vai trò là các bit chuẩn để luân chuyển dữ liệu trên Ethernet.



Hình 1.3. Các thành phần của Ethernet

1.2.5. Hoạt động của Ethernet

Các máy Ethernet (còn được gọi là máy trạm) hoạt động độc lập với tất cả các trạm khác trên mạng và không có một trạm điều khiển trung tâm.

1.2.6. Sự khác nhau giữa Internet và Ethernet

Ethernet:

Công nghệ mạng được coi là tiêu chuẩn nhất hiện nay và được sử dụng trong hầu hết các công ty kinh doanh. Ethernet cho phép truyền dữ liệu dạng chuỗi với tốc độ 10 megabit mỗi giây, với thông số thực tế từ 2 đến 3 megabit mỗi giây.

Internet

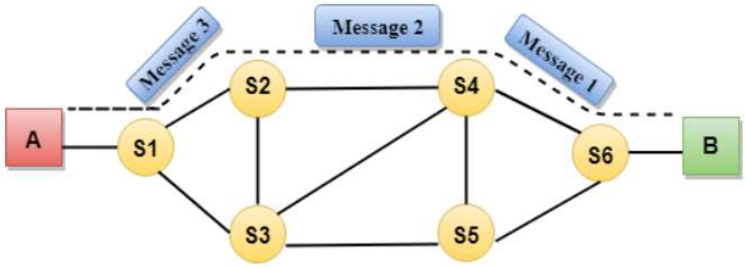
Hệ thống bao gồm các máy tính trong một mạng được kết nối với nhau trên toàn thế giới, cho phép các dịch vụ truyền dữ liệu như đăng nhập từ xa, truyền và gửi tập tin email. Internet là một cách kết nối các mạng máy tính để bạn có thể nhìn thấy bức tranh toàn cảnh về cách thức hoạt động của từng hệ thống.

1.3. Kỹ thuật chuyển mạch trong mạng nội bộ

1.3.1. Khái niệm chuyển mạch

Chuyển mạch:

- Chuyển mạch kênh là một kỹ thuật chuyển mạch thiết lập một đường dẫn riêng giữa người gửi và người nhận. Trong Kỹ thuật chuyển mạch, một khi kết nối được thiết lập thì đường dẫn dành riêng sẽ vẫn tồn tại cho đến khi kết nối bị ngắt. Chuyển mạch kênh trong mạng hoạt động theo cách tương tự như hoạt động của điện thoại. Một đường dẫn end-to-end hoàn chỉnh phải tồn tại trước khi quá trình giao tiếp diễn ra.



Hình 1.4. Giao tiếp thông qua chuyển mạch

1.3.2. Các công nghệ chuyển mạch

Chuyển mạch phân chia không gian:

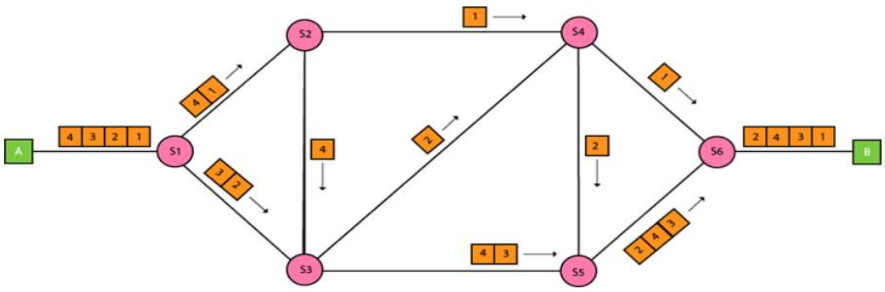
Chuyển mạch phân chia không gian là một công nghệ chuyển mạch kênh trong đó một đường truyền duy nhất được thực hiện trong một bộ chuyển mạch bằng cách sử dụng một tập hợp các điểm chéo riêng biệt về mặt vật lý.

Chuyển mạch thông điệp

Chuyển mạch thông điệp là một kỹ thuật chuyển mạch trong đó thông điệp được chuyển như một đơn vị hoàn chỉnh và được định tuyến qua các nút trung gian mà tại đó nó được lưu trữ và chuyển tiếp.

Chuyển mạch gói

Chuyển mạch gói là một kỹ thuật chuyển mạch trong đó thông điệp được gửi trong một lần, nhưng nó được chia thành nhiều phần nhỏ hơn và chúng được gửi riêng lẻ. Nếu bất kỳ gói nào bị thiếu hoặc bị hỏng, thì thông báo sẽ được gửi đi để gửi lại tin nhắn. Nếu đạt được thứ tự chính xác của các gói, thì thông báo xác nhận sẽ được gửi.



Hình 1.5. Chuyển mạch gói

1.4. Kết luận Chương 1

Kết thúc Chương 1, luận văn đã nghiên cứu tổng quan về mạng nội bộ và các kỹ thuật sử dụng trong mạng nội bộ, bao gồm: khái niệm mạng nội bộ, lợi ích của mạng nội bộ, khá niệm về công nghệ Ethernet và các kỹ thuật liên quan. Ngoài ra, luận văn cũng đã nghiên cứu và tìm hiểu về chuyển mạch và một số công nghệ chuyển mạch.

Từ những nghiên cứu về mạng nội bộ và các kỹ thuật chuyển mạch, học viên nhận thấy mạng nội bộ có cấu trúc rất phức tạp và có nhiều thiết bị cấu thành một mạng nội bộ. Đồng thời các kỹ thuật chuyển mạch cũng rất đa dạng và tồn tại nhiều nhược điểm. Điều này dẫn đến việc nguy cơ bị tấn công mạng thông qua các thiết bị thành phần và trong chính các kỹ thuật chuyển mạch, định tuyến. Chính vì vậy vì vậy, cần phải nghiên cứu các phương thức tấn công mạng nội bộ để đưa ra giải pháp phòng chống.

CHƯƠNG 2: TẤN CÔNG MẠNG NỘI BỘ VÀ GIẢI PHÁP PHÒNG CHỐNG

2.1. Tổng quan về an toàn bảo mật thông tin

An ninh mạng ngày càng trở nên quan trọng hơn khi điện thoại thông minh, máy tính và máy tính bảng trở thành một phần không thể thiếu trong công việc hàng ngày và cuộc sống cá nhân. Mức độ phụ thuộc vào các công cụ trực tuyến trong các khía cạnh khác nhau của hoạt động kinh doanh – từ mạng xã hội và tiếp thị qua email đến lưu trữ dữ liệu nhân viên và khách hàng trên đám mây – đặt ra nhu cầu bổ sung trong việc bảo vệ những thông tin quý giá này.

Khi ngày càng có nhiều công ty nhận thức được tầm quan trọng của việc bảo vệ tài nguyên của họ và thực hiện đào tạo về an ninh mạng, thì tin tặc và tội phạm mạng cũng đang phát triển các hình thức tấn công khác ngày càng tinh vi hơn.

Có năm loại tấn công mạng phổ biến nhất: Malware, Phishing, Denial of Service (DoS), Man in the middle (MitM), Zero-day attack.

2.2. Một số kỹ thuật tấn công mạng nội bộ

2.2.1.Tấn công sử dụng phần mềm độc hại (Malware)

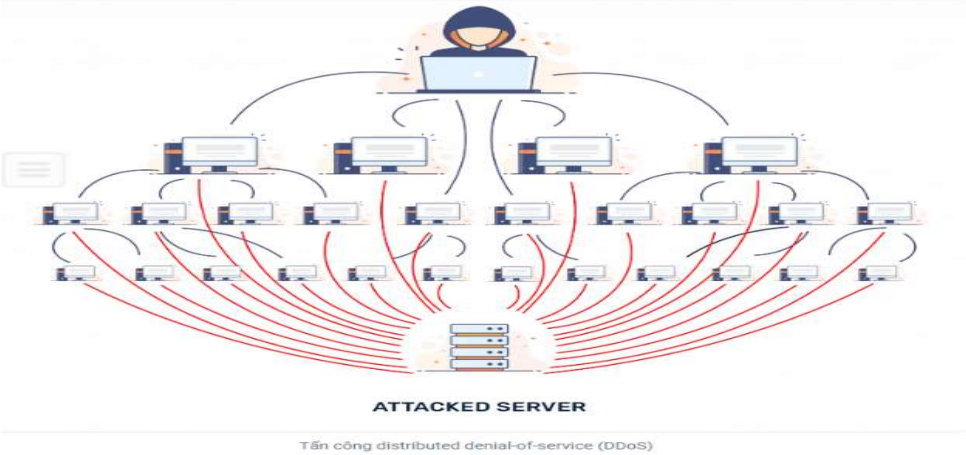
Các cuộc tấn công bằng phần mềm độc hại là hình thức phổ biến và phổ biến nhất. Chúng bao gồm phần mềm gián điệp (gián điệp), ransomware (mã độc) và sâu (phần mềm độc hại có thể lây lan sang các thiết bị khác). Những kẻ tấn công thường sử dụng các lỗ hổng bảo mật để nhắm mục tiêu người dùng.

2.2.2. Tấn công giả mạo (Phishing)

Phishing là một kiểu tấn công chiếm được lòng tin của người dùng bằng cách mạo danh một cá nhân hoặc tổ chức hợp pháp, thường thông qua tin nhắn văn bản hoặc email.

2.2.3. Tấn công từ chối dịch vụ (DoS và DDoS)

Một cuộc tấn công DDos sẽ chiếm đoạt tài nguyên (resource) của hệ thống khiến nó không thể phản hồi các yêu cầu dịch vụ. Cuộc tấn công DDoS cũng là một cuộc tấn công vào tài nguyên của hệ thống, nhưng nó được thực hiện từ một số lượng lớn các host khác mà bị nhiễm phần mềm độc hại do hacker kiểm soát.



Hình 2.1. Tấn công DDoS

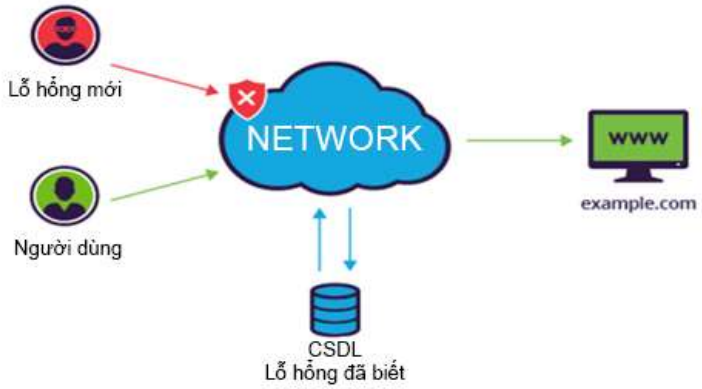
2.2.4. Tấn công cơ sở dữ liệu (SQL injection)

Kẻ tấn công " tiêm " một đoạn mã độc hại vào cơ sở dữ liệu sử dụng ngôn ngữ truy vấn có cấu trúc(SQL), mục đích là khiến máy chủ trả về những thông tin quan trọng mà không được tiết lộ. Các cuộc tấn công SQL injection được xuất phát từ lỗ hổng của website.

Hình 2.2. Tấn công cơ sở dữ liệu

2.2.5. Khai thác lỗ hổng Zero-day (Zero day attack)

Lỗ hổng Zero-day (hay còn gọi là 0-day vulnerabilities) là các lỗ chưa được công bố, các nhà cung cấp phần mềm chưa biết tới do đó chưa có bản vá chính thức. Do đó, việc khai thác các lỗ hổng mới như vậy là cực kỳ nguy hiểm và không thể đoán trước, đồng thời có thể gây ra hậu quả nghiêm trọng cho người dùng và chính nhà xuất bản sản phẩm.

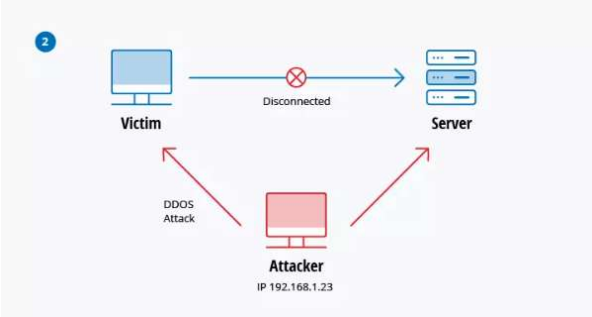


Hình 2.3. Khai thác lỗ hổng Zero-day

2.2.6. Tấn công Man in the middle (MitM)

Một tấn công MitM xảy ra khi một hacker tự chèn vào giữa các giao tiếp của client và server. Dưới đây là một số kiểu tấn công man-in-the-middle phổ biến:

Session hijacking (chiếm quyền điều khiển)



Hình 2.4. Tấn công Man in the middle

2.2.7. Các loại khác

Ngoài ra, còn có nhiều hình thức tấn công mạng khác như tấn công chuỗi cung ứng, tấn công email, v.v. Mỗi hình thức tấn công đều có những đặc điểm riêng, ngày càng phức tạp và tinh vi buộc các cá nhân, tổ chức phải thường xuyên cảnh giác và luôn cập nhật các công nghệ phòng chống mới.

2.3. Một số giải pháp phòng chống tấn công mạng nội bộ

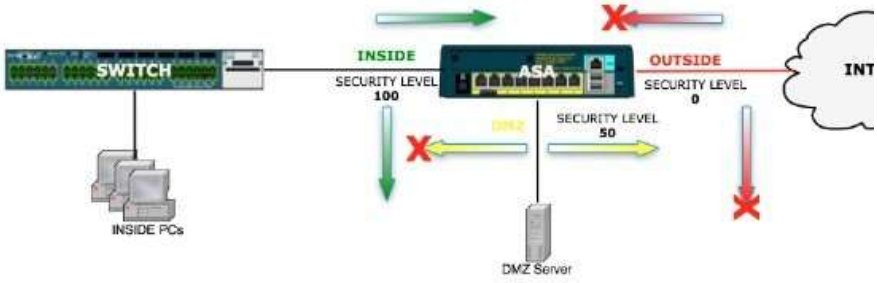
2.3.1. Sử dụng tường lửa (Firewall)

2.3.1.1. Khái niệm

Firewall là thuật ngữ xuất phát từ trong phòng cháy chữa cháy công trình xây dựng, người ta đã thiết kế ra các bức tường có chức năng chống cháy lan. Thuật ngữ này được áp dụng vào an toàn thông tin, Firewall có tác dụng là một hệ thống phòng thủ, bảo vệ dữ liệu khỏi sự tấn công, và là "chốt chặn", kiểm soát thông tin ra vào hệ thống, hạn chế những truy cập trái phép.

2.3.1.2. Tường lửa cứng

Tường lửa cứng hay Hardware Firewall là thuật ngữ chỉ các thiết bị phần cứng có chức năng kiểm tra tất cả các dữ liệu đi qua và chặn các gói dữ liệu nguy hiểm, hoặc các truy cập không mong muốn. Tường lửa cứng thường được đặt tại phía ngoài của mạng nội bộ, đón dữ liệu từ ngoài trước khi được đưa vào trong mạng nội bộ.



Hình 2.5. Mô tả cơ bản vị trí của tường lửa cứng trong mạng

2.3.1.3. Tường lửa mềm

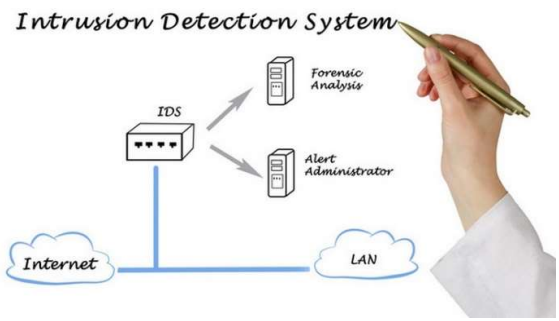
Tường lửa mềm là các phần mềm có chức năng kiểm soát truy cập từ bên ngoài, chặn các truy cập trái phép, các mã độc, v.v…

Hình 2.6. Phần mềm tường lửa AVS Firewall

2.3.2. Công nghệ phát hiện và ngăn chặn xâm nhập IDS/IPS

2.3.2.1. Phát hiện xâm nhập IDS

Hệ thống phát hiện xâm nhập IDS (Intrusion Detection System) là những phần mềm, công cụ có khả năng giám sát mạng, phát hiện những bất thường, các hành vi trái phép, cố gắng xâm nhập vào hệ thống.



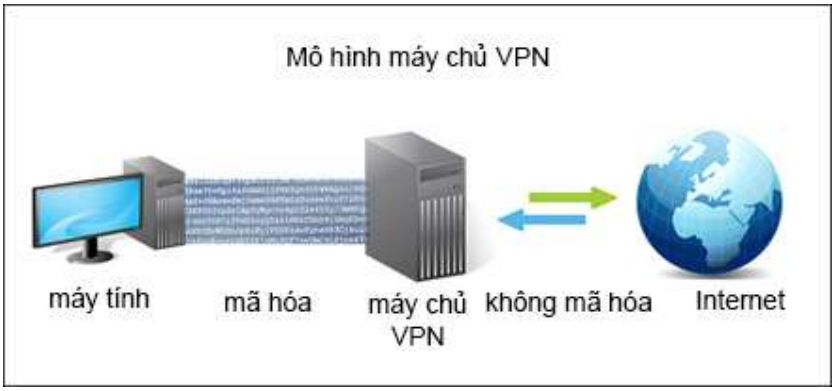
Hình 2.7. Mô hình diễn tả hệ thống IDS

2.3.2.2. Ngăn chặn xâm nhập IPS

Hệ thống ngăn chặn xâm nhập IPS (Intrusion Prevention System) là những phần mềm, công cụ có khả năng theo dõi, ngăn chặn kịp thời những hành vi tấn công, xâm nhập mạng nội bộ.

2.3.3. Mạng riêng ảo VPN

Mạng riêng ảo VPN – Virtual Private Network tạo ra các kết nối mạng riêng tư giữa các thiết bị trên môi trường Intranet. VPN được dùng để gửi nhận dữ liệu một cách an toàn và ẩn danh qua các mạng công cộng.



Hình 2.8. Mô hình VPN

2.3.4. Mạng LAN ảo VLAN

Mạng LAN ảo VLAN – Virtual Local Area Network là một nhóm các thiết bị mạng và thiết bị đầu cuối, được gom lại một cách logic, dựa theo các yếu tố đặc trưng như chức năng, bộ phận, vị trí địa lý, ứng dụng…

2.3.5. Các biện pháp khác

2.4. Kết luận Chương 2

Trong Chương 2, luận văn đã trình bày một số vấn đề như: tổng quan về an toàn và bảo mật thông tin, một số kỹ thuật tấn công mạng nội bộ phổ biến như: Malware, Phising, DoS và DDoS, SQL injection, Zero-day attack, MitM. Ngoài ra luận văn còn đưa ra một số giải pháp chống tấn công mạn nội bộ như Firewall, IDS/IPS, VPN, VLAN và một số biện pháp liên quan đến yếu tố con người.

Tuy nhiên do các phương pháp tấn công ngày càng tinh vi và liên tục thay đổi, nên việc phòng chống cũng vì vậy mà gặp nhiều khó khan, do đó cần có sự thử nghiệm và đánh giá.

CHƯƠNG 3: THỰC NGHIỆM VÀ ĐÁNH GIÁ

3.1. Phần mềm hỗ trợ thực nghiệm

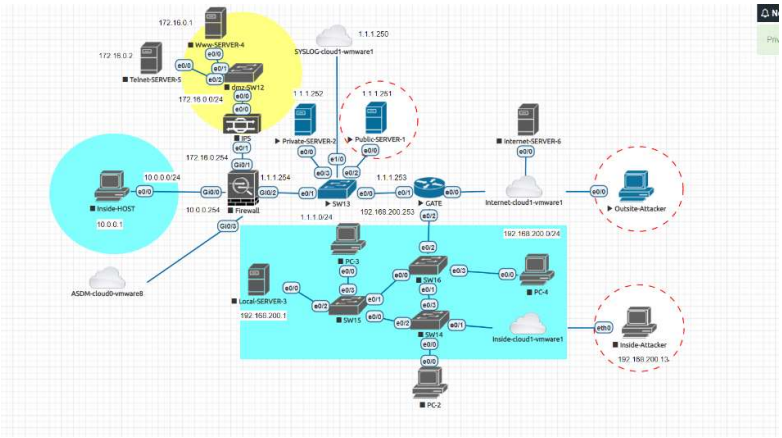
3.1.1. Công cụ giả lập EVE-NG

EVE-NG (viết tắt của Emulated Virtual Environment – Next Generation)là một trong các công cụ giả lập (emulator) tốt nhất hiện nay. Cùng các tính năng của UnetLab , Eve-ng có thể giả lập được rất nhiều loại thiết bị mạng đang được sử dụng rộng rãi như router, switch của Cisco, Juniper, v.v…

3.1.2. Hệ điều hành Kali Linux

Hệ điều hành Kali Linux cung cấp giải pháp thử nghiệm tấn công rất tốt đối với các mô hình giả lập. Với các thư viện có sẵn, việc thử nghiệm tấn công sẽ diễn ra rất nhanh chóng, không mất quá nhiều thời gian chuẩn bị, từ đó có thể tập trung vào việc kiểm tra lỗ hổng của hệ thống và tìm phương án phòng thủ.

3.2. Cài đặt và triển khai mô hình



Hình 3.1. Mô hình thử nghiệm

3.3. Kịch bản thử nghiệm

Tấn công nội bộ theo 3 kịch bản:

- ✓ MAC-Overflow.
- ✓ ARP- Poisoning.

Tấn công từ bên ngoài vào hệ thống:

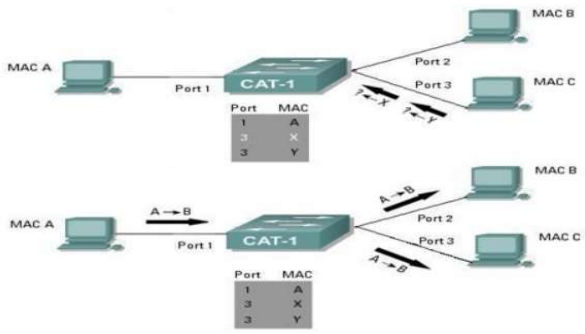
- ✓ Access-Cracking.

3.3. Tiến hành tấn công và phòng thủ trên mô hình thử nghiệm

3.3.1. Kỹ thuật tấn công MAC-Overflow

3.3.1.3. Tấn công làm tràn bảng MAC

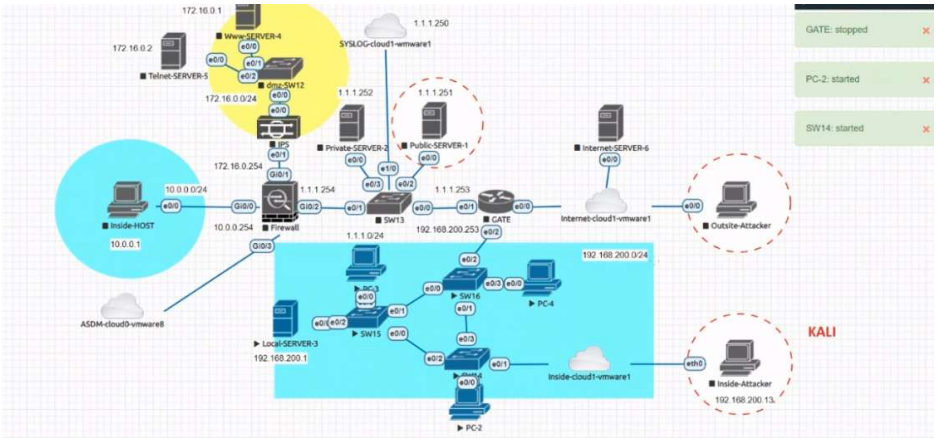
Tấn công làm tràn bảng MAC dựa vào điểm yếu của thiết bị chuyển mạch cụ thể là thiết bị Switch: bảng MAC chỉ có thể chứa được một số hữu hạn các ánh xạ (như switch Catalysh 6000 có thể chứa tối đa là 128.000 ánh xạ) và các ánh xạ này không phải tồn tại mãi trong bảng MAC.



Hình 3.2. Minh họa bảng MAC

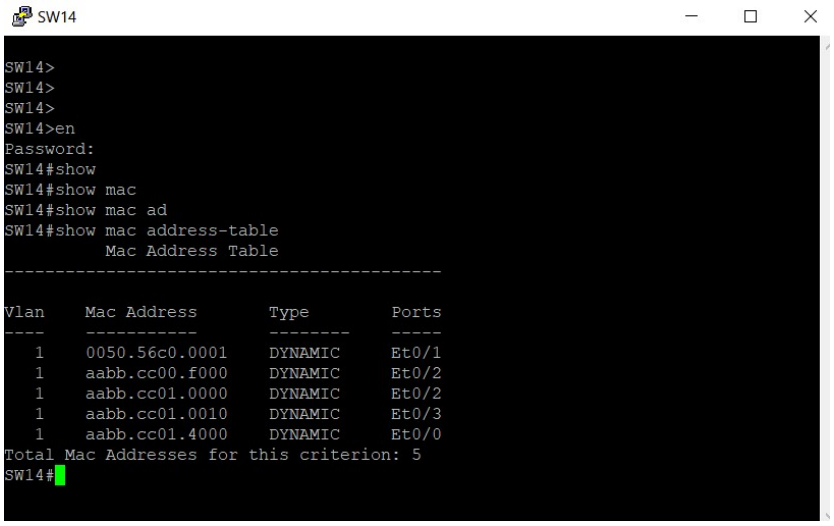
3.3.1.4. Phương thức tấn công MAC-Overflow

Attacker nằm bên trong sau khi đã chiếm quyền hoặc nhân viên đã bị mua chuộc , gián điệp trực tiếp tấn công từ bên trong vùng inside:



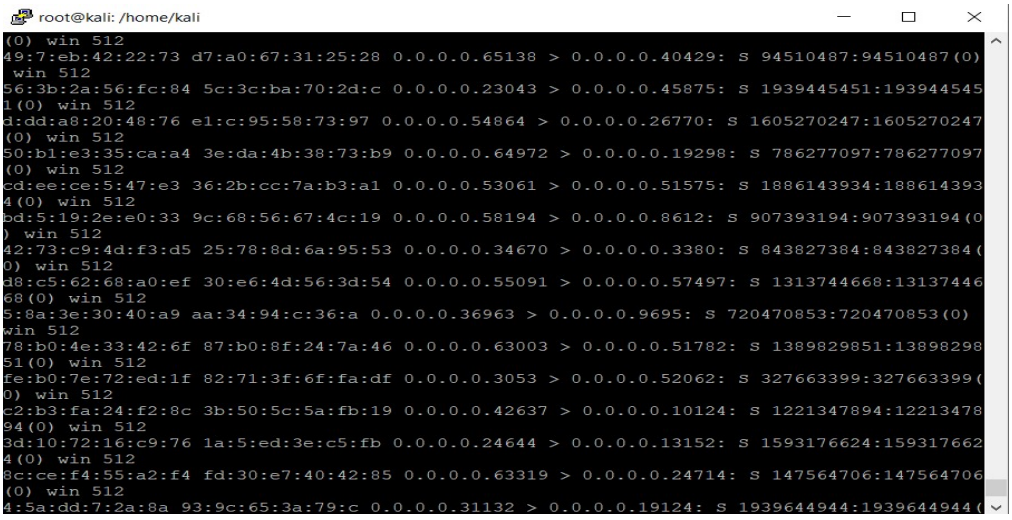
Hình 3.3. Sơ đồ tổng quan kịch bản MAC Overflow trên Eve-ng

Bảng MAC trước khi bị tấn công :



Hình 3.4. Hiển thị bảng MAC thiết bị SW14 ban đầu

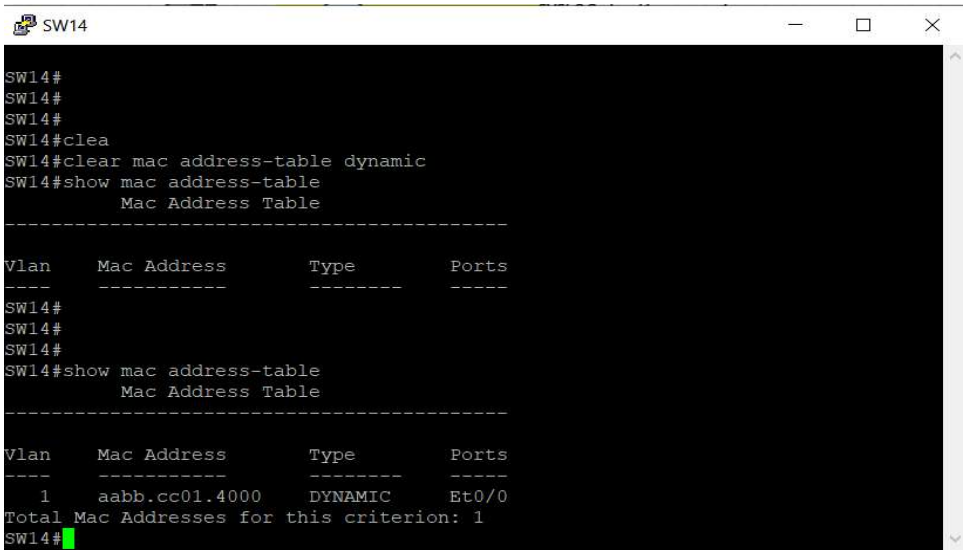
Xuất hiện các MAC giả mạo được Kali gửi liên tục :



Hình 3.5. Máy attacker gửi liên tục các địa chỉ MAC giả mạo

Ta thấy xuất hiện rất nhiều MAC giả mạo traffic từ cổng E0/1:

- Sử dụng câu lệnh clear dể xoá các MAC giả mạo



Hình 3.6. Clear bảng MAC trên SW14

3.3.1.5 Giải pháp phòng vệ

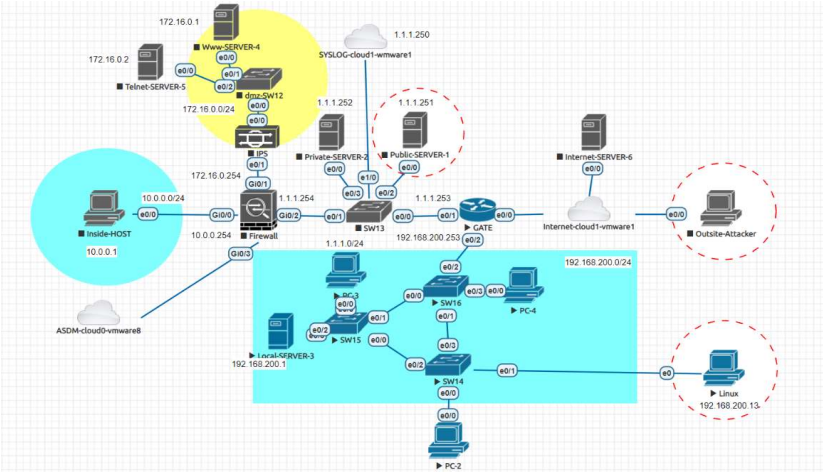
Giải pháp ta sử dụng port security bằng câu lệnh cho SW4 :

Giải pháp port security trên một cổng này chỉ cho 1 số lượng MAC nhất định nào đó để kết nối vào và nếu có nhiều MAC gửi kết nối và sẽ shutdown cổng:

3.3.2. Kỹ thuật tấn công ARP-Poisoning

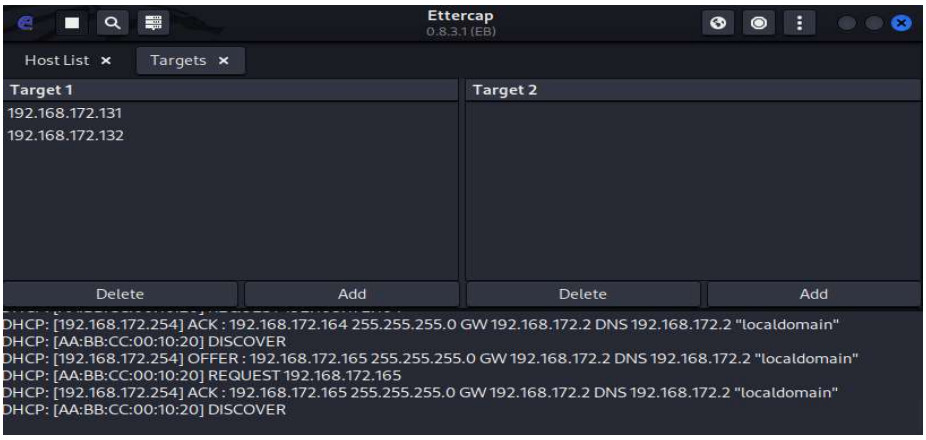
3.3.2.1. Lỗ hổng của ARP

ARP (viết tắt của Address Resolution Protocol) là một giao thức truyền thông được sử dụng phổ biến để tìm ra các địa chỉ tầng liên kết dữ liệu từ các địa chỉ mạng.



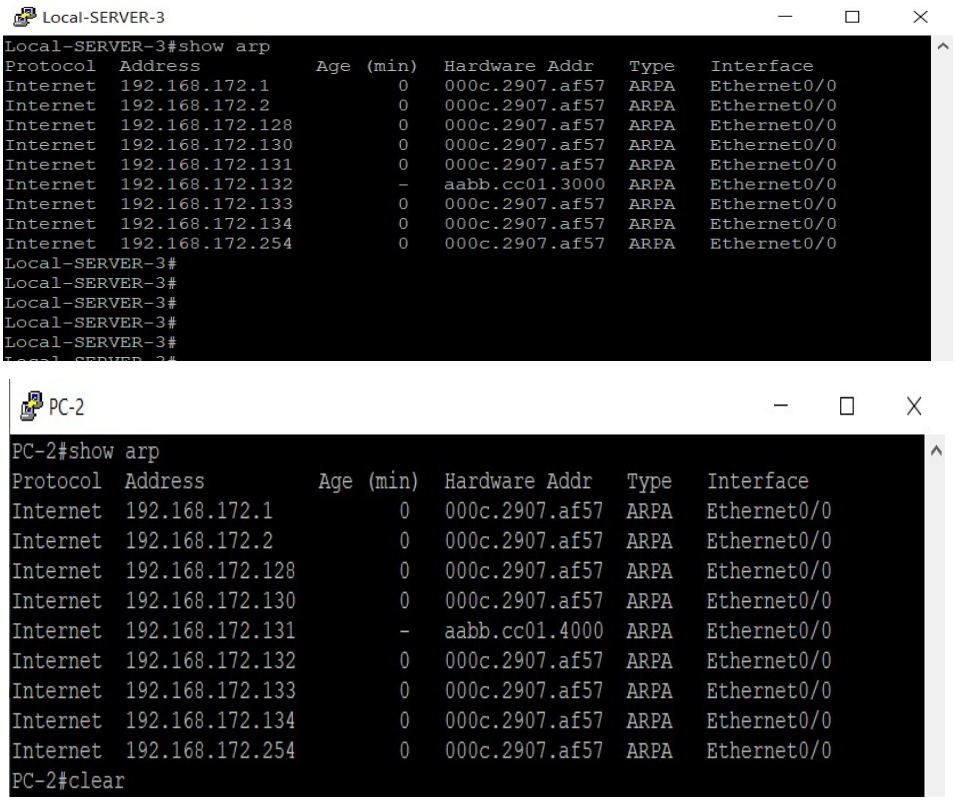
Hình 3.7. Sơ đồ bài lab tấn công ARP-Poisoning

Theo sơ đồ trên ta tập trung cho 2 thiết bị là PC-2, Local-Server-3 và thiết bị GATE đóng vai trò là máy chủ DHCP cấp phát ip lần lượt là Local-SERVER-3: 192.168.172.131 và PC-2: 192.168.172.132. Tiếp theo từ máy Kali ta thực hiện tấn công ARP-Poisoning với công cụ Ettercap:



Hình 3.8. Trên máy attacker add 2 mục tiêu PC2 và Local Server3

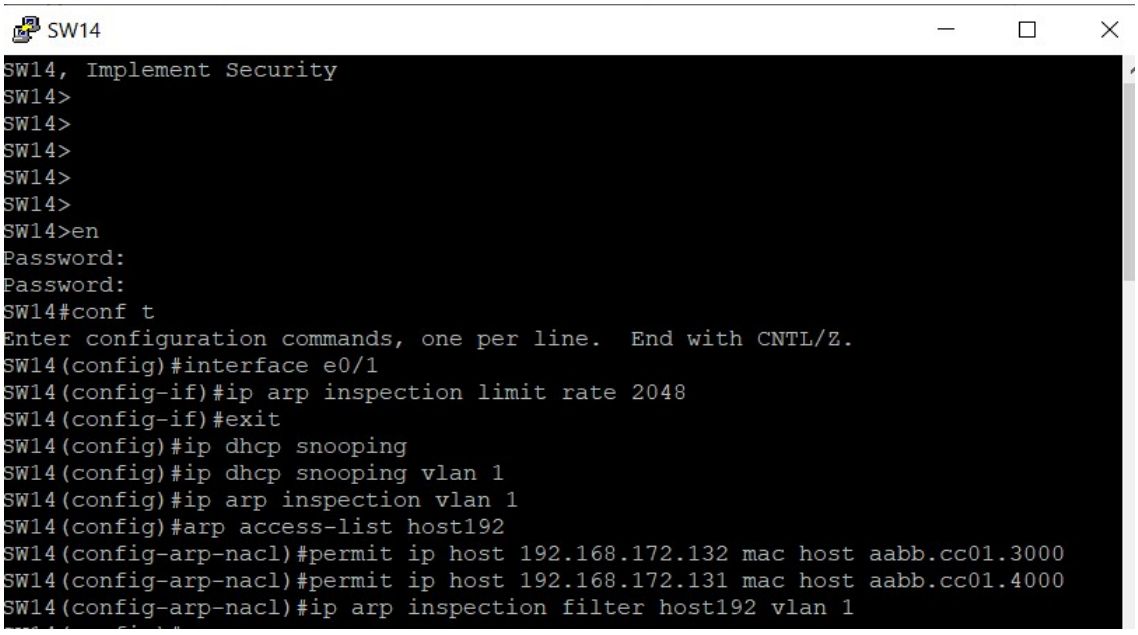
Sau khi thực hiện tấn công, ta xem thông tin arp của 2 thiết bị nạn nhân đều thấy các thiết bị cùng 1 địa chỉ MAC, ở đây chính là địa chỉ MAC của máy Kali:



Hình 3.9. Kiểm tra bảng MAC của các thiết bị nạn nhân

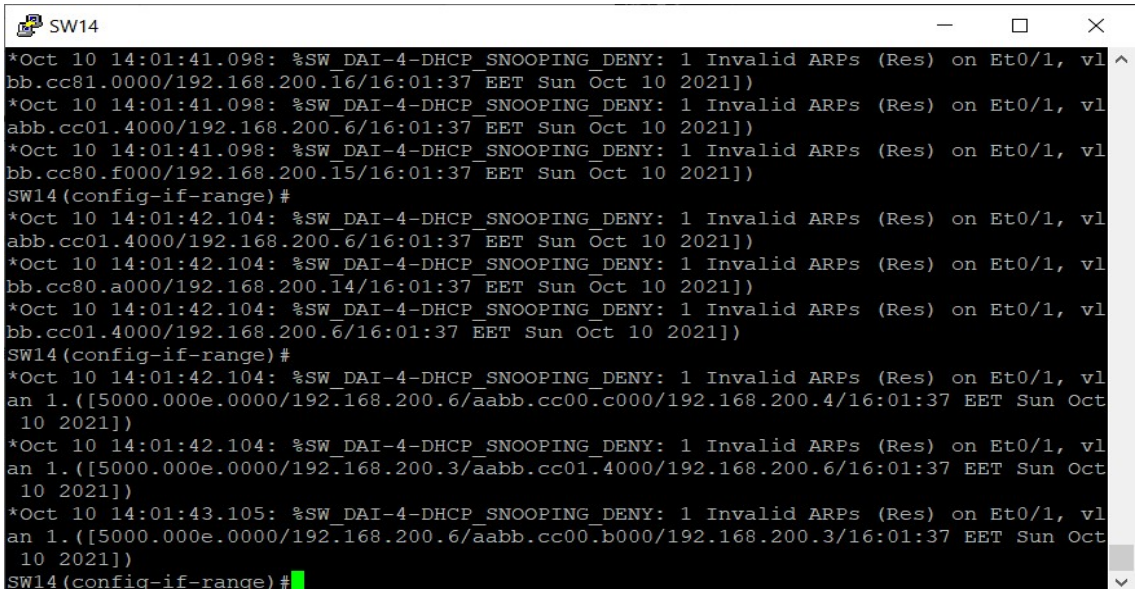
3.3.2.3. Giải pháp

Giải pháp ở đây là ta sử dụng ip snooping trên Switch14 với mục đích là chặn các gói arp giả mạo của kẻ tấn công. Cấu hình trên SW14 như sau:



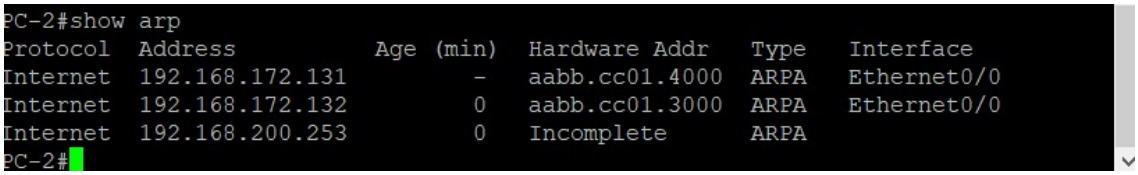
Hình 3.10. Cấu hình ip snooping trên SW14 để phòng vệ

Sau khi cấu hình máy kali thực hiện tấn công lại sẽ xuất hiện các dòng thông báo chặn gói ARP của cổng e0/1 SW14:

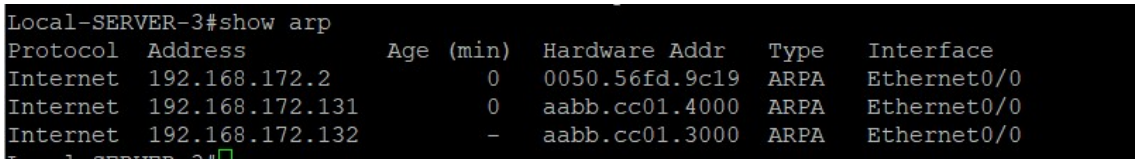


Hình 3.11. Tấn công lại lần nữa từ máy Attacker thấy SW14 hiện cảnh báo

Và địa chỉ MAC của 2 thiết bị PC-2 và Local-SERVER-3 không bị thay đổi



Hình 3.12. Kiểm tra lại bảng Mac của thiết bị PC2 thấy bình thường



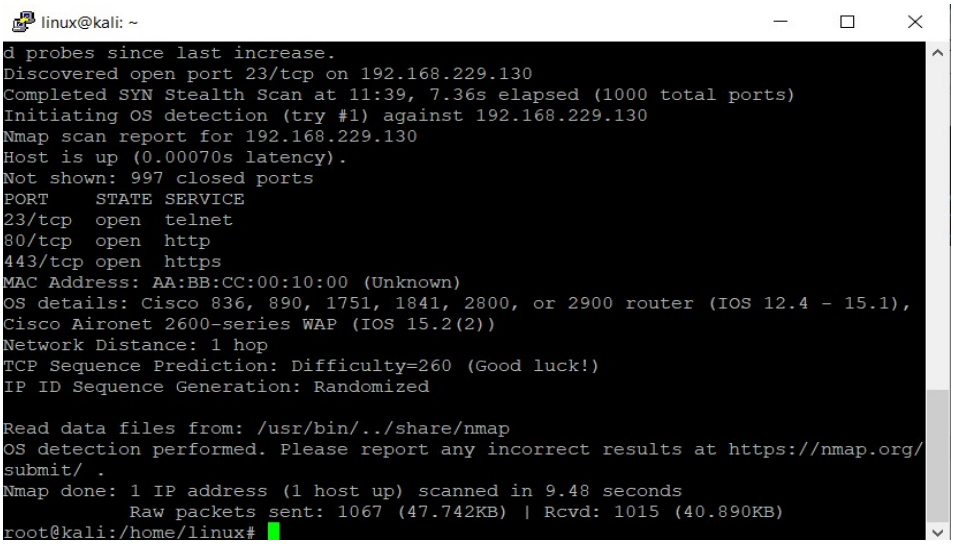
Hình 3.13. Kiểm tra lại bảng Mac của thiết bị Local-Server3 thấy bình thường

3.3.3. Phương thức tấn công Access-Cracking

Việc hệ thống mục tiêu sử dụng các cấu hình được thiết lập mặc định bởi nhà sản xuất thiết bị phần cứng hay phần mềm làm cho việc tấn công vào mục tiêu đó trở nên dễ dàng hơn bao giờ hết.

3.3.3.1. Tấn công Access-Cracking

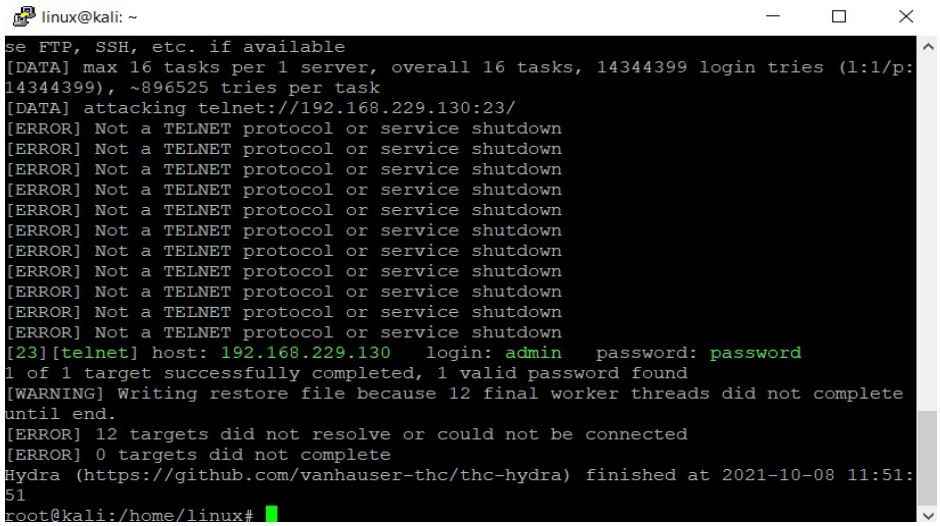
Kiểu tấn công này mục đích là do thám các thiết bị bên trong hệ thống mạng sử dụng kỹ thuật Nmap để dò được các thông tin về thiết bị, phiên bản, hệ điều hành,… và sau đó tiến hành dò tài khoản mật khẩu sử dụng Hydra để bẻ khóa mật khẩu.



Hình 3.14. Sử dụng Nmap dò thông tin của thiết bị thông qua IP

Phát hiện được router mở cổng 23 telnet máy kali thực hiện dò tài khoản mật khẩu để xâm nhập bằng cách nhập câu lệnh như sau:

hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz telnet://192.168.229.130



Hình 3.15. Dò thành công tài khoản và mật khẩu để truy cập vào thiết bị GATE

3.3.3.2 Giải pháp

Giải pháp cho kiểu tấn công này là ta thực hiện lắp thiết bị tường lửa và cấu hình đúng các luật để chặn các lưu lượng trái phép truy cập vào hệ thống mạng hoặc vận hành thiết bị router tích hợp tính năng của Firewall và cấu hình các chính sách cụ thể không cho phép các thiết bị bên ngoài có thể giao tiếp được đến Router.

3.4. Hướng phát triển

Sau khi đã thực hiện thành thạo các công cụ trên hệ điều hành Kali Linux và trau dồi được kỹ năng lập trình với ngôn ngữ Python thì hoàn toàn có thể xây dựng riêng một ứng dụng hoặc một trang web để sử dụng pentest cho hệ thống. Hoặc có thể tập hợp các công cụ đánh giá an toàn thông tin cho người dùng với mục đích học tập dễ sử dụng, tham khảo và triển khai tại nơi làm việc.

3.5. Kết luận Chương 3

Trong Chương 3, luận văn đã trình bày phần thực nghiệm mô phỏng tấn công và chống tấn công với 3 phương thức.

- ✓ MAC-Overflow.
- ✓ ARP- Poisoning.
- ✓ Access-Cracking.

Đồng thời với mỗi phương pháp tấn công, học viên đã trình bày phương pháp để phòng chống và thực nghiệm phòng chống, kết quả đạt được là đã ngăn được phương pháp tấn công đó. Từ đó cho thấy hiệu quả của công tác phòng chống tấn công trong mạng nội bộ.

KẾT LUẬN

Trong phạm vi nghiên cứu, luận văn đã giới thiệu tổng quan về mạng nội bộ, một số công nghệ lõi sử dụng trong mạng nội bộ. Giới thiệu sơ bộ về các phương pháp tấn công vào một mạng nội bộ, đồng thời đưa ra một số giải pháp để phòng chống tấn công. Dựa trên cơ sở đó để tiến hành thực nghiệm mô phỏng hệ thống mạng nội bộ và thực hiện tấn công bằng 03 phương pháp tấn công mạng (02 phương pháp tấn công từ bên trong và 01 phương pháp tấn công từ bên ngoài).

Bám sát theo mục tiêu và nhiệm vụ của đề tài, luận văn đã thu được một số kết quả như:

- ✓ Mô phỏng được mô hình mạng thiết kế trên công cụ EVE-NG.
- ✓ Tìm hiểu được các lỗ hổng về mặt cấu hình cũng như các kiểu tấn công phổ biến.
- ✓ Thành thạo một số công cụ có sẵn trên hệ điều hành Kali Linux.
- ✓ Đưa ra được các giải pháp ngăn chặn các cuộc tấn công.

Những hạn chế còn tồn tại

- ❖ Do kinh nghiệm thực tế chưa được nhiều, kiến thức về lỗ hổng còn hạn chế, và thời gian có hạn, do vậy chưa khai thác được thêm nhiều các kiểu tấn công mới.
- ❖ Chưa vận dụng được nhiều công cụ để tạo ra mã khai thác hoặc công cụ không có sẵn để thực hiện tấn công và phòng chống.

TÀI LIỆU THAM KHẢO

Tiếng Anh

[1] D Son, Sooel; Shmatikov, Vitaly (August 14, 2017). *"The Hitchhiker's Guide to DNS Cache Poisoning"* (PDF). Cornell University. Archived (PDF) from the original on.

[2] Ramachandran, Vivek & Nandi, Sukumar (2005). *"Detecting ARP Spoofing: An Active Technique"*. In Jajodia, Suchil & Mazumdar, Chandan (eds.). Information systems security: first international conference, ICISS 2005, Kolkata, India, Birkhauser. p. 239. ISBN 978-3-540-30706-8. Computer Network.

[3] Forouzan, Behrouz (February 17, 2012). *"Data Communications and Networking. McGraw-Hill"*. p. 14. ISBN 9780073376226.

[4] Gary A. Donahue (June, 2007). *"Network Warrior"*. O'Reilly.

[5] Stoneburner, G.; Hayden, C.; Feringa, A. (2004). *"Engineering Principles for Information Technology Security"*. csrc.nist.gov.doi:10.6028/NIST.SP.800-27rA

[6] Yehuda Afek, Anat Bremler-Barr, Alon Noy – (October 2, 2019), *"Eradicating Attacks on the Internal Network with Internal Network Policy"*

[7] Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). *"Towards a More Representative Definition of Cyber Security"*. Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

Website

[1] https://www.msspalert.com/cybersecurity-guests/multi-vector-attacks-demand-multi-vector-protection/

[2] https://www.rapid.7.com/fundarmentals/vulnerabilities-exploits-threats/